Department of Defense
DIRECTIVE

March 21, 1988
NUMBER 5200.28

USD(A)

SUBJECT: Security Requirements for Automated Information Systems (AISs)

References: (a) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972 (hereby canceled)
(b) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
(c) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981
(d) DoD Directive S-5200.19, "Control of Compromising Emanations (U)," February 10, 1968
(e) through (v), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive:

1. Reissues and revises reference (a) to update uniform policy in addition to the policy set forth in reference (b) for the safeguarding of classified, sensitive unclassified, and unclassified information processed in AISs.

2. Updates the DoD-wide program for Automated Information System (AIS) security.

3. Provides mandatory, minimum AIS security requirements. More stringent requirements may be necessary for selected systems based on an assessment of acceptable levels of risk.

4. Promotes the use of cost-effective, computer-based (e.g., hardware, software, and firmware controls) security features for AISs. However, it is emphasized that system users have a personal responsibility to protect classified information under subparagraph 10-101.a. of reference (b).

5. Requires a more accurate specification of overall DoD security requirements for AISs that process classified or sensitive unclassified information.

6. Stresses the importance of a life-cycle management approach to implementing computer security requirements.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments and the Military Services within those Departments,

the Joint Chiefs of Staff (JCS), the Joint Staff, the Unified and Specified Commands, the Defense Agencies, the DoD Field Activities, and such other offices, Agencies, activities, and commands as may be established or designated by law, by the President, or by the Secretary of Defense (hereafter referred to collectively as "DoD Components").

2. This Directive applies to the following classes of information:

a. Classified information. Thereby, supplementing DoD 5200.1-R (reference (b)) for such information when contained in the AISs.

b. Sensitive unclassified information.

c. Unclassified information.

3. This Directive applies to all AISs including stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; embedded computer systems; communications switching computers; personal computers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, as may be developed.

4. This Directive, reference (b), and DoD Directive C-5200.5 (reference (c)) apply to transmission and communications media connecting components of or to an AIS.

5. This Directive, DoD Directive S-5200.19 (reference (d)), NACSI 5004 (reference (e)), and NACSI 5005 (reference (f)) apply to the emanations security requirements of AISs.

6. This Directive and DCID No. 1/16 (reference (g)) apply to AISs processing foreign intelligence and/or counterintelligence information.

7. This Directive and SM-313-83 (reference (h)) apply to AISs processing Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).

8. This Directive and DoD Instruction 5215.2 (reference (i)) apply to the reporting and dissemination of AIS technical vulnerabilities and corrective measures.

9. All AISs that handle classified, sensitive unclassified, or unclassified information shall comply with the pertinent requirements of this Directive. Unless otherwise required by the Designated Approving Authority (DAA), AISs that meet any of the following conditions shall be excluded from meeting policy subsections D.5. through D.7., below, of this Directive:

a. AISs that are operated only in the dedicated security mode.

b. Personal computers, word processors, and similar stand-alone AISs in which it technically is not feasible to configure the equipment to support internal security controls. Such AISs may be characterized as being single-state machines without a privileged instruction set or memory lock features, and shall be operated only in the dedicated mode.

c. An AIS that is embedded in a larger system and is not removed easily, is without users, and normally receives input from, or gives output only to, other parts of the system.

10. AIS networks must be examined on a case-by-case basis for application of policy in this Directive. The DAA for the network should obtain guidance through established command channels, from the National Security Agency (NSA), or where applicable, from the Defense Intelligence Agency (DIA) on evaluation and accreditation (see enclosure 5).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD policy that:

1. Classified information and sensitive unclassified information shall be safeguarded at all times while in AISs. Safeguards shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required. When classified information is involved, the information security requirements in DoD 5200.1-R (reference (b)) shall be met.

2. Unclassified information while in AISs shall be safeguarded against tampering, loss, and destruction and shall be available when needed. This is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse. Suggested safeguards for unclassified information are in OMB Circular No. A-130 (reference (j)), and include applicable personnel, physical, administrative, and technical controls.

3. The safeguarding of information and AIS resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection.

4. The mix of safeguards selected for an AIS that processes classified or sensitive unclassified information shall ensure the AIS meets the minimum requirements as set forth in enclosure 3. These minimum requirements shall be met through automated and manual means in a cost-effective and integrated manner. An analysis shall be performed using enclosure 4 to identify any additional requirements over and above the set of minimum requirements.

5. Computer security features of commercially produced products and Government-developed or -derived products shall be evaluated (as requested) for designation as trusted computer products for inclusion on the Evaluated Products List (EPL). Evaluated products shall be designated as meeting security criteria

maintained by the National Computer Security Center (NCSC) at NSA defined by the security division, class, and feature (e.g., B, B1, access control) described in DoD 5200.28-STD (reference (k)).

6. The following timetable shall be adhered to:

a. All AISs that process or handle classified and/or sensitive unclassified information and that require at least controlled access protection (i.e., class C2 security), based on the risk assessment procedure described in enclosure 4, shall implement required security features by 1992.

b. If security features above class C2 are required for an AIS, based on the risk assessment procedure described in enclosure 4, a timetable for meeting these more stringent requirements shall be determined on an individual system basis and submitted to the DAA for approval. These requirements shall be met either by implementing trusted computer products listed on the EPL or by using a product not on the EPL that has security features that meet the level of trust required for the AIS. In either case, to assess whether adequate security measures have been taken to permit the AIS to be used operationally, an accreditation must be accomplished and approved by the cognizant DAA.

7. There are cases where introduction of additional computer-based security features, according to the schedule given in subsection D.6., above, for an existing AIS or an AIS already under development, may be prohibitively expensive, time-consuming, unsound technically, or adversely may impact operational effectiveness to an unacceptable degree. In such cases, the following shall apply:

a. Other safeguards (e.g., physical controls, administrative controls, etc.) may be substituted as long as the requisite level of system security or protection, as determined by the DAA, is attained.

b. Exceptions to subsection D.6., above, may be authorized only by the DoD Component Head, or a senior DAA appointed by the DoD Component Head. Such authorization shall be based on a written determination that one or more of the conditions of subsection D.7., above, exists. Exceptions shall be reviewed at each reaccreditation.

8. When AISs managed by different DAAs are interfaced or networked, a memorandum of agreement (MOA) is required that addresses the accreditation requirements for each AIS involved. The MOA should include description and classification of the data; clearance levels of the users; designation of the DAA who shall resolve conflicts among the DAAs; and safeguards to be implemented before interfacing the AISs. MOAs are required when one DoD Component's AIS interfaces with another AIS within the same DoD Component or in another DoD Component and when a contractor's AIS interfaces with a DoD Component's AIS or to another contractor's AIS.

a. For a multi-user telecommunications network (e.g., the Defense Data Network or the World Wide Military Command and Control System Intercomputer

Network), a DAA shall be designated as responsible for the overall security of the network and shall determine the security and protection requirements for connection of AISs to the network.

b. Necessary safeguards shall be agreed to and implemented and the AISs accredited for interconnection before they are connected to the network.

c. The security of each AIS connected to the network remains the responsibility of its DAA.

d. The DAA responsible for the overall security of the network shall have the authority and responsibility to remove from the network any AIS not adhering to the security requirements of the network.

e. It is permissible to define network interfaces and boundaries into manageable subnetworks based upon physical or logical boundaries, when there is a need to do so. Cryptographic separation and/or equivalent computer security measures, as defined by the NSA or the DIA where applicable, shall be a basis for defining such network and/or subnetwork interfaces or boundaries.

f. Networks, including all connected subnetworks, shall be accredited for the highest division and class of security required based on the concepts and procedures in enclosures 4 and 5.

9. Security policy shall be considered throughout the life cycle of an AIS from the beginning of concept development, through design, development, operation, and maintenance until replacement or disposal. A DAA shall be designated as responsible for the overall security of the AIS. The following conditions shall be met:

a. The AIS developer is responsible for ensuring the early and continuous involvement of the users, information system security officers, data owners, and DAA(s) in defining and implementing security requirements of the AIS. There shall be an evaluation plan for the AIS showing progress towards meeting full compliance with stated security requirements through the use of necessary computer security safeguards.

b. Mandatory statements of safeguard requirements shall be included, as applicable, in the acquisition and procurement specifications for AISs. The statements shall be the result of an initial risk assessment, and shall specify the level of trust required under DoD 5200.28-STD (reference (k)).

c. No classified or sensitive unclassified data shall be introduced into an AIS without designation of the classification and sensitivity of the data. Approval to enter the data shall be obtained from the data owner where applicable.

d. The accreditation of an AIS shall be supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report, all approved by the DAA. Accreditation of computers embedded in a system may be at the system level.

e. A program for conducting periodic reviews of the adequacy of the safeguards for operational, accredited AISs shall be established. To the extent possible, reviews are to be conducted by persons who are independent of the user organization and of the AIS operation or facility.

f. Where required, as specified in OMB Circular No. A-130 (reference (j)), a program for developing and testing contingency plans shall be established. The objective of contingency planning is to provide reasonable continuity of AIS support if events occur that prevent normal operations. The plans should be tested periodically under realistic operational conditions.

g. Changes affecting the security of an AIS must be anticipated. Any changes to the AIS or associated environment that affect the accredited safeguards or result in changes to the prescribed security requirements shall require reaccreditation. Reaccreditation shall take place before the revised system is declared operational. Minimally, an AIS shall be reaccredited every 3 years, regardless of changes.

10. Access by foreign nationals to a U.S. Government-owned or U.S. Government-managed AIS may be authorized only by the DoD Component Head, and shall be consistent with the Department of Defense, the Department of State (DoS), and the Director of Central Intelligence (DCI) policies.

11. An AIS accredited to process and/or store Sensitive Compartmented Information (SCI) may use automated means (software, firmware, or hardware) to permit classified non-SCI data to be extracted from the SCI system for use at the non-SCI classified level. This capability is permissible only if it was considered and approved as part of the security accreditation and the AIS is operating at a minimum security class of B1.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C^3I)) shall:

a. Oversee and review implementation of this Directive.

b. Develop overall AIS security policies and procedures in accordance with U.S. national policies and Directives in coordination with the Under Secretary of Defense (Policy) (USD(P)), and consistent with DoD policies under DoD 5200.1-R (reference (b)), DoD Directive 7920.1 (reference (l)), DCID No. 1/16 (reference (g)), and DoD Instruction 5210.74 (reference (m)).

c. Promulgate Instructions, Standards, Manuals, and other issuances, as required, in accordance with this Directive.

d. Represent the Department of Defense on interagency committees engaged in development of security policy, standards, and criteria for AISs.

2. The Deputy Under Secretary of Defense (Policy) (DUSD(P)) shall continue to review, oversee, and formulate overall policies that govern DoD security

practices and programs, to include developing, coordinating, and presenting DoD positions on the following:

a. Information Security.

b. Physical Security.

c. Personnel Security.

d. Industrial Security.

3. The Director, Defense Investigative Service (DIS), shall implement an AIS security program for DoD contractor AISs in accordance with DoD Directive 5220.22 (reference (n)) and DoD 5220.22-R (reference (o)).

4. The Director, Defense Communications Agency (DCA), shall implement an AIS security program for long-haul communication systems that do not handle SCI and shall certify devices that perform secured or protected telecommunications switching functions.

5. The Director, Defense Intelligence Agency (DIA), shall implement a program for the security of DoD Component and DoD contractor AISs and networks (e.g., the DoD Intelligence Information System network) that handle SCI. The program shall not apply to AISs and networks under the cognizance of the National Security Agency and/or the Central Security Service (NSA/CSS).

6. The National Security Agency and/or the Central Security Service (NSA/CSS) shall:

a. Implement an AIS security program for all AISs under NSA/CSS jurisdiction, including those of NSA/CSS contractors.

b. As requested, provide DoD Components with communications and computer security assistance and advice in support of effective AIS security measures.

c. Establish and maintain technical standards and criteria for evaluating and certifying trusted computer products. Review, at least yearly, DoD 5200.28-STD (reference (k)) and provide recommendations for revision to the ASD(C^3I).

d. Provide training for DoD Components in evaluation techniques and procedures as applicable to reference (k), and certify such DoD Components to conduct evaluations.

e. Evaluate computer products intended for use by DoD Components or contractors as trusted computer products. These evaluations may be conducted on computer products developed or derived by either industry or Government sources. Also, perform quality assurance and certify evaluations performed by DoD Components.

f. Maintain and publish the EPL of evaluated industry and Government-developed or -derived trusted computer products.

g. Conduct, approve, and sponsor research and development of techniques and equipment for trusted computer products and for computer security evaluation and verification methods and techniques.

h. Serve as the focal point for technical matters on using trusted computer products and systems and, with DoD Component computer security testing and evaluation activities, provide technical advice to the DoD Components on using trusted products and systems.

i. Ensure that AIS security posture assessments, made in accordance with the DoD computer security program, are incorporated into NCSC goals and objectives.

j. Annually assess the overall AISs security posture and disseminate information on hostile threats against DoD AISs.

k. Operate a central technical center to provide, as requested, technical assistance to evaluate and certify the computer-based security features of AISs used in operational environments.

l. Prescribe the minimum security standards, methods, and procedures for safeguarding an AISs classified and sensitive technical security material, techniques, and information.

m. Review and approve standards, techniques, systems, and equipments for telecommunications and automated information systems security.

7. The Joint Chiefs of Staff (JCS) shall:

a. Implement an AIS security program under this Directive and SM-313-83 (reference (h)) for AISs of DoD Components and their contractors that handle SIOP-ESI.

b. Provide a source of education and training for managers in AIS security through the Department of Defense Computer Institute (DoDCI) of the National Defense University (NDU) (DoD Directive 5200.2 (reference (p))).

8. The Heads of DoD Components shall:

a. Implement and maintain an overall AIS security program designed to ensure compliance with this Directive.

b. Ensure that contractual requirements to protect classified and sensitive unclassified information are provided to their contractors.

c. Ensure that funding and resources are programmed for staffing, training, and supporting for this AIS security program and for implementation of AISs safeguards, as required, within the DoD Component.

d. Assign official(s) as the DAA (e.g., senior AIS policy official) responsible for accrediting each AIS under his or her jurisdiction and for ensuring compliance with AIS security requirements.

e. Establish and maintain an AIS security training and awareness program for all DoD military, civilian, and contractor personnel requiring access to AISs.

f. Ensure that periodic independent reviews of the security and protection of their AISs are done to ensure compliance with stated AIS security goals. Such reviews may be done using the procedures in DoD Directive 5010.38 (reference (q)).

g. Support the Computer Security Technical Vulnerability Reporting Program in accordance with DoD Instruction 5215.2 (reference (i)).

9. Each Designated Approving Authority (DAA) shall:

a. Review and approve security safeguards of AISs and issue accreditation statements for each AIS under the DAA's jurisdication based on the acceptability of the security safeguards for the AIS.

b. Ensure that all the safeguards required, as stated in the accreditation documentation for each AIS, are implemented and maintained.

c. Identify security deficiencies and, where the deficiencies are serious enough to preclude accreditation, take action (e.g., allocate additional resources) to achieve an acceptable security level.

d. Ensure that an Information System Security Officer (ISSO) is named for each AIS, and that he or she receives applicable training to carry out the duties of this function. It is recommended that the ISSO not report to operational elements of the AIS over which security requirements of this Directive must be enforced.

e. Require that an AIS security education and training program be in place.

f. Ensure that data ownership is established for each AIS, to include accountability, access rights, and special handling requirements.

10. Each Information System Security Officer (ISSO) shall:

a. Ensure that the AIS is operated, used, maintained, and disposed of in accordance with internal security policies and practices.

b. Have the authority to enforce security policies and safeguards on all personnel having access to the AIS for which the ISSO has cognizance.

c. Ensure that users have the required personnel security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with internal security practices before access to the AIS.

d. Ensure that audit trails are reviewed periodically.

e. Begin protective or corrective measures if a security problem exists.

f. Report security incidents in accordance with DoD 5200.1-R (reference (b)) and to the DAA when an AIS is involved.

g. Report the security status of the AIS, as required by the DAA.

h. Evaluate known vulnerabilities to ascertain if additional safeguards are needed.

i. Maintain a plan for system security improvements and progress towards meeting the accreditation.

F. EFFECTIVE DATE AND IMPLEMENTATION

1. This Directive is effective immediately.

2. Accreditations made using the requirements of the previous version of this Directive remain valid, but shall be updated within 3 years from the date of this Directive.

3. AISs that have started the design phase of the life-cycle process before the date of this Directive shall be accredited within 3 years of that date or before initial operational capability.

4. Each DoD Component Head shall forward an implementation plan for compliance with this Directive to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C^3I)) within 180 days of the date of this Directive. This Directive shall be implemented without new DoD Component issuances.

William H. Taft, IV
Deputy Secretary of Defense

Enclosures - 5
1. References
2. Definitions
3. Minimum Security Requirements
4. Procedure for Determining Minimum AIS Computer-Based Security Requirements
5. Network Considerations

REFERENCES, Continued

(e) National Communication Security Instruction 5004, "TEMPEST Countermeasures for Facilities Within the United States." January 1, 1984
(f) National Communication Security Instruction 5005, "TEMPEST Countermeasures for Facilities Outside the United States," January 1, 1984
(g) Director of Central Intelligence Directive Number 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks (U)," January 4, 1983
(h) SM-313-83, "Safeguarding the Single Integrated Operational Plan (U)," May 10, 1983
(i) DoD Instruction 5215.2, "Computer Security Technical Vulnerability Reporting Program," September 2, 1986
(j) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," December 12, 1985
(k) DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985, authorized by DoD Directive 5200.28, December 18, 1972
(l) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)," October 17, 1978
(m) DoD Instruction 5210.74, "Security of DoD Contractor Telecommunications," June 26, 1985
(n) DoD Directive 5220.22, "Industrial Security Program," November 1, 1986
(o) DoD Regulation 5220.22-R, "Industrial Security Regulation," December 1985, authorized by DoD Directive 5220.22, December 8, 1980
(p) DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979
(q) DoD Directive 5010.38, "Internal Management Control Program," July 16, 1984
(r) Executive Order 12356, "National Security Information," April 6, 1982
(s) DoD Directive 5230.24, "Distribution Statement on Technical Documents," March 18, 1987
(t) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by DoD Directive 5200.28, December 18, 1972
(u) CSC-STD-003-85, "Computer Security Requirements," June 25, 1985
(v) NCSC-TG-005, Version 1, "Trusted Network Interpretations," July 31, 1987

DEFINITIONS

1. Access. A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an AIS resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information.

2. Accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions.

3. Accreditation. A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

4. AIS Security. Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data, and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

5. Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation.

6. Audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

7. Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

8. Automated Information Systems (AISs). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

9. Category. A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that

personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information).

10. Certification. The technical evaluation of an AISs security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements.

11. Classified Information. Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356 (reference (r)), or prior orders, DoD 5200.1-R (reference (b)), to require protection against unauthorized disclosure; and (c) so designated.

12. Computer. A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices.

13. Data. A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an AIS.

14. Data Integrity. The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed.

15. Data Owner. The authority, individual, or organization who has original responsibility for the data by statute, Executive order, or Directive.

16. Dedicated Security Mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories.

17. Denial of Service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability.

18. Designated Approving Authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirments of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS.

19. Embedded System. An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands, or fire control systems).

20. Evaluated Products List (EPL). A documented inventory of equipments, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD (reference (k)).

21. Features. (See Security Features, definition 40., below.)

22. Formal Access Approval. Documented approval by a data owner to allow access to a particular category of information.

23. Handled By. The term "handled by" denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating, and controlling.

24. Information. Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

25. Information System. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

26. Information System Security Officer (ISSO). The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal.

27. Intelligent Terminal. A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics.

28. Multilevel Security Mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS.

29. Need-to-Know. A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services.

30. Network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

31. Orange Book Terminology. Reference (k), also called the Orange Book, classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and B there are further subdivisions called classes. These classes also are ordered in a hierarchical manner characterized by the set of computer security features they possess (see Security Features, definition 40., below).

32. Partitioned Security Mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in DCID No. 1/16, reference (g).

33. Periods Processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period.

34. Purge. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is ensurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge.

35. Risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

36. Risk Analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

37. Risk Index. The disparity between the minimum clearance or authorization of AIS users and the maximum sensitivity (e.g., classification and categories) of data handled by the AIS.

38. Risk Management. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk anslysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

39. Safeguards. (See Security Safeguards, definition 42., below.)

40. Security Features. The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, access control).

41. Security Mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS.

42. Security Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

43. Sensitive Compartmented Information (SCI). Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence.

44. Sensitive Unclassified Information. Any information the loss, misuse, or unauthorized access to, or modification of which, adversely might affect U.S national interest, the conduct of DoD programs, or the privacy of DoD personnel (e.g., FOIA exempt information and information whose distribution is limited by DoD Directive 5230.24 (reference (s))).

45. SIOP-ESI. An acronym for Single Integrated Operational Plan-Extremely Sensitive Information, a DoD Special Access Program.

46. Special Access Program. Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know.

47. System High Security Mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

48. Telecommunications. Under this Directive, a general term expressing data transmission between computing systems and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission.

49. Trusted Products. Products evaluated and approved for inclusion on the Evaluated Products List (EPL).

50. Unclassified Information. Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse.

51. Users. People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

MINIMUM SECURITY REQUIREMENTS

A. MINIMUM SECURITY REQUIREMENTS. The following minimum requirements shall be met through automated or manual means in a cost-effective manner and integrated fashion:

1. Accountability. There shall be in place safeguards to ensure each person having access to an AIS may be held accountable for his or her actions on the AIS. There shall be an audit trail providing a documented history of AIS use. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur. To fulfill this requirement, the manual and/or automated audit trail shall document the following:

a. The identity of each person and device having access to the AIS.

b. The time of the access.

c. User activity sufficient to ensure user actions are controlled and open to scrutiny.

d. Activities that might modify, bypass, or negate safeguards controlled by the AIS.

e. Security relevent actions associated with periods processing or the changing of security levels or categories of information.

DAAs shall cause a review to be made of audit trails associated with the AIS(s) over which the DAAs have cognizance to determine an adequate retention period for the audit information. The decision to require an audit trail of user access to a stand-alone, single-user AIS (e.g., personal computer (PC), memory typewriter, drafting machine) should be left to the discretion of the DAA.

2. Access. There shall be in place an access control policy for each AIS. It shall include features and/or procedures to enforce the access control policy of the information within the AIS. The identify of each user authorized access to the AIS shall be established positively before authorizing access.

3. Security Training and Awareness. There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS. The program shall ensure that all persons responsible for the AIS and/or information, therein, and all persons who access the AIS are aware of proper operational and security-related procedures and risks.

4. Physical Controls. AIS hardware, software, and documentation, and all classified and sensitive unclassified data handled by the AIS shall be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification (i.e., data integrity shall be maintained). The level of control and protection shall be commensurate with the maximum sensitivity of the information and shall provide the most restrictive control measures required by the data to be handled. This includes having personnel, physical, administrative, and configuration controls. Additionally, protection against denial of service of AIS resources (e.g., hardware, software, firmware, and information) shall be

consistent with the sensitivity of the information handled by the AIS. Unclassified hardware, software, or documentation of an AIS shall be protected if access to such hardware, software, or documentation reveals classified information, or access provides information that may be used to eliminate, circumvent, or otherwise render ineffective the security safeguards for classified information. Software development and related activities (e.g., systems analysis) shall be controlled by physical controls (e.g., two-person control) and protected when it is determined that the software shall be used for handling classified or sensitive unclassified data.

5. Marking. Classified and sensitive unclassified output shall be marked to accurately reflect the sensitivity of the information. Requirements for security classification and applicable markings for classified information are set forth in DoD 5200.1-R (reference (b)). The marking may be automated (i.e., the AIS has a feature that produces the markings) or may be done manually. Automated markings on output must not be relied on to be accurate, unless the security features and assurances of the AIS meet the requirements for a minimum security class B1 as specified in DoD 5200.28-STD (reference (k)). If B1 is not met, but automated controls are used, all output shall be protected at the highest classification level of the information handled by the AIS until manually reviewed by an authorized person to ensure that the output was marked accurately with the classification and caveats. All media (and containers) shall be marked and protected commensurate with the requirements for the highest security classification level and most restrictive category of the information ever stored until the media are declassified (e.g., degaussed or erased) using a DoD-approved methodology set forth in the DoD AIS Security Manual, DoD 5200.28-M (reference (t)), or unless the information is declassified or downgraded in accordance with reference (b).

6. Least Privilege. The AIS shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but to no more. In the case of "need-to-know" for classified information, access must be essential for accomplishment of lawful and authorized Government purposes.

7. Data Continuity. Each file or data collection in the AIS shall have an identifiable source throughout its life cycle. Its accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know.

8. Data Integrity. There shall be safeguards in place to detect and minimize inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.

9. Contingency Planning. Contingency plans shall be developed and tested in accordance with OMB Circular No. A-130 (reference (j)) to ensure that AIS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data is modified or destroyed, procedures must be in place to recover.

10. Accreditation. Each AIS shall be accredited to operate in accordance with a DAA-approved set of security safeguards.

11. Risk Management. There should be in place a risk management program

to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.

PROCEDURE FOR DETERMINING MINIMUM AIS COMPUTER-BASED SECURITY REQUIREMENTS

A. RISK ASSESSMENT PROCEDURE. The following risk assessment procedure is extracted from CSC-STD-003-85 (reference (u)). The procedure is used to determine the minimum evaluation class required for an AIS, based on the sensitivity of the information present in the AIS and on the clearances of its users. Any DoD Component desiring to use a different method to accomplish the intent of this enclosure may do so, if prior approval has been granted by the ASD(C^3I).

NOTE: In the case of a network, the procedure is applied individually to each of the AISs in the network. The resulting evaluation class should be taken as a minimum partial requirement since connection of an AIS to another AIS or to a network may result in additional risks (see enclosure 5). The DAA for a network also may decide to apply the procedure once for the network, and determine the evaluation class by applying the requirements in DoD 5200.28-STD (reference (k)) to the network as a whole.

1. Step 1. Determine System Security Mode of Operation. The system security mode of operation for an AIS is determined as follows:

a. An AIS is defined as operating in the dedicated security mode if all users have the clearance or authorization, documented formal access approval, if required, and the need-to-know for all information handled by the AIS. The AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. The AIS shall be isolated electrically, logically, and physically from all personnel and AISs not possessing the requisite clearance or authorization, formal access approval, if required, and need-to-know for all of the information handled by the AIS.

b. An AIS is defined as operating in the system high security mode if all users have the clearance or authorization and documented formal access approval, if required, but not necessarily the need-to-know for all information handled by the AIS.

c. An AIS is defined as operating in the multilevel security mode if not all users have the clearance, authorization, or formal access approval, if required, for all information handled by the AIS.

d. An AIS is defined as operating in the partitioned security mode if all users possess the clearance, but not necessarily a formal access approval, for all information handled by the AIS.

2. Step 2. Determine Minimum User Clearance or Authorization Rating. The minimum user clearance or authorization (Rmin) is defined as the maximum clearance or authorization of the least cleared or authorized user. Rmin is determined from Table 1. The clearances used in the following table are defined in DoD Directive 5200.2 (reference (p)).

TABLE 1

MINIMUM USER CLEARANCE OR AUTHORIZATION SCALE

	Rating
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or Current Background Investigation (BI)	4
Top Secret (TS) and/or Current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

3. Step 3. Determine Maximum Data Sensitivity Rating. The maximum data sensitivity (Rmax) is determined from the following table:

TABLE 2

MAXIMUM DATA SENSITIVITY SCALE

Maximum Sensitivity Ratings 2/ Without Categories (Rmax)	Rating (Rmax)	Maximum Data Sensitivity With Categories 1/		Rating (Rmax)
Unclassified (U)	0	Not Applicable 3/		
Not Classified but Sensitive 4/	1	N	With One or More Categories	2
Confidential (C)	2	C	With One or More Categories	3
Secret (S)	3	S	With One or More Categories With No More Than One Category Containing Secret Data	4
		S	With Two or More Categories Containing Secret Data	5
Top Secret (TS)	5 5/	TS	With One or More Categories With No More Than One Category Containing Secret or Top Secret Data	6
		TS	With Two or More Categories Containing Secret or Top Secret Data	7

1/ The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data is in the same category are treated as without categories.

2/ Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

3/ Unclassified data by definition may not contain categories.

4/ Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. Table 2 prescribes minimum ratings.

5/ The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage.

4. Step 4. Determine Risk Index. The risk index depends on the rating associated with the AIS minimum user clearance (Rmin) and the rating associated with the maximum classification of the information handled by the AIS (Rmax).

The risk index is computed as follows:

a. Case a. If Rmin is less than Rmax, then the risk index is determined by subtracting Rmin from Rmax.

Risk Index = Rmax - Rmin

NOTE: There is one anomalous value that results because there are two "types" of Top Secret clearance and only one "type" of Top Secret data. When the minimum user clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1, which should result from a straight application of the formula).

b. Case b. If Rmin is greater than or equal to Rmax, then:

Risk Index = 1, if there are categories to which some users are not authorized access, or:

Risk Index = 0, in all other cases.

5. Step 5. Determine Minimum Security Evaluation Class For Computer-Based Controls.

a. The following table shall be used to determine the minimum security class required for an AIS based on the computed risk index in Step 4, above. The levels in the table are those described in DoD 5200.28-STD (reference (k)).

TABLE 3

COMPUTER SECURITY REQUIREMENTS SCALE

Risk Index	Security Mode	Minimum Security Class 4/
0	Dedicated 5/	No minimum class 1/, 2/
0	System High	C2 2/
1	Multilevel, Partitioned	B1 3/
2	Multilevel, Partitioned	B2
3	Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

1/ Although there is no prescribed minimum class, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

2/ Automated markings on output must not be relied on to be accurate unless at least class B1 is used. (See requirements for marking in enclosure 3.)

3/ Where an AIS handles classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being handled, at least a class B2 is required.

4/ The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

5/ Most embedded systems and desk top computers operate in the dedicated mode.

6. Step 6. Adjustments to Computed Security Evaluation Class Required. Additional requirements or recommendations relevant to determining the minimum evaluation class include the following:

a. Where an AIS is connected to a network or to another AIS, care should be taken to ensure that the requirements for accreditation of the AIS are not violated due to the presence of the network technology.

b. In the dedicated mode where the AIS is connected to a network or to another AIS, it is recommended (although not required) that at least level C1 be used. This recommendation is made because level C1 might provide a measure of security sufficient to prevent users from accidentally altering or deleting each other's data.

c. An AIS using periods processing (i.e., operating in one or more security modes and/or at one or more security levels for certain periods of

time where acceptable sanitization procedures are implemented between processing periods) may have more than one risk index. In such cases, the highest value of risk index shall be used in determining the minimum security feature level.

NETWORK CONSIDERATIONS

A. For purposes of accreditation, a network shall be treated as either an interconnection of accredited AISs (which may be networks) or as a unified network. These two cases are discussed below:

1. Case I. Interconnections of Accredited AISs

a. If a network consists of previously accredited AISs, an MOA is required between the DAA of each DoD Component AIS and the DAA responsible for the network (as provided in section D. of this Directive). The network DAA must ensure that interface restrictions and limitations are observed for connections between DoD Component AISs. The NCSC-TG-005 (reference (v)) provides interface restriction and limitation that may be applicable. In particular, connections between accredited AISs must be consistent with the mode of operation of each AIS, the specific sensitivity level or range of sensitivity levels for which each AIS is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.

b. Each AIS shall be assigned an accreditation range, consisting of the set of security levels that may be associated with data it sends over the network connection. If the accreditation range is more than a single level, the AIS reliably must segregate data by level within its accreditation range, and label it accurately for transmission over multilevel interfaces.

c. DAAs of DoD Component AISs should be aware that connection to a network may involve additional risks because of the potential exposure of data in their own AIS to the larger community of all users of AISs in the network. In connections to adjacent AISs, the operational modes and security mechanisms of those AISs should be taken into consideration, beyond the simple fact of their accreditation.

d. Untrusted, unaccredited AISs, either individual computer systems or subnetworks, also may be components of a network. Connections between them and other component AISs are permissible under the same conditions in paragraph A. 1.a., above. Only unclassified information, which does not include sensitive unclassified information, may be sent to and from the untrusted, unaccredited AISs.

e. Special AISs for support, such as packet switching nodes and terminal access interfaces, also must have received individual accreditation if they carry classified or sensitive unclassified information. The network DAA serves as the DAA for all such AISs.

2. Case II. Unified Networks

a. Some networks may be accredited as a whole without prior accreditation of each of their component AISs. It is necessary to treat a network as unified when some of its component AISs are so specialized or dependent on other components of the network for security support that individual accreditation of such components is not possible or meaningful with respect to secure network operation. In order to be accredited, a unified network shall possess a coherent

network security architecture and design, and it should be developed with an attention to security requirements, mechanisms, and assurances commensurate with the range of sensitivity of information for which it is to be accredited.

b. The recommended approach for accrediting a unified network is to apply enclosure 4 to the entire network to derive an evaluation class. Requirements to meet that evaluation class then are obtained from an applicable interpretation of DoD 5200.28-STD (reference (k)), such as NCSC-TG-005 (reference (v)).